SECTION 6

Electric and Electronic Security Devices

6.1 Introduction

The previous sections of this document identified applications for which utilities may want to install electric and electronic security devices. A utility's decision to use this equipment should be based on its DBT, as well as other operational and design considerations. This section provides an overview of issues and situations that should be considered when determining what type of electric or electronic security system to install once a decision has been made that a such a system will be employed. Included are descriptions of security devices, including intrusion detection systems, access control and card readers, biometric readers, and closed-circuit surveillance camera systems. Lighting and wiring are also discussed.

A variety of different security systems and components are commercially available. Before specifying and purchasing any security devices, it is important to understand the characteristics and requirements of the area and facility to be protected. With this understanding in hand, detailed criteria can be developed to specify exactly how the device should be implemented and how the device fits into the overall security system.

6.2 System Considerations

To determine the type of security system to install, it is important to understand the characteristics of the area to be protected, as well as the security expectations and requirements. This section describes the information that should be obtained and questions that should be asked to help a utility plan and implement a security system.

6.2.1 Threat

As mentioned previously, the types of security equipment employed will be dependent on a utility's DBT. The utility must understand from whom it is trying to protect the space. Questions that the utility needs to consider include:

- Is the anticipated adversary an outsider, an insider, or an outsider collaborating with an insider?
- What tactics, motivation, skills, knowledge, tools or weapons might the adversary use? Protecting a facility from a skilled, trained terrorist with knowledge of the facility requires a different tactic than protecting against a teen-aged vandal.

6.2.2 Known Vulnerabilities and Key Assets

A utility's vulnerability assessment will identify the assets that are most critical to meeting its mission. The types of assets to be protected will influence the type of equipment recommended to protect them.

6.2.3 Areas of Coverage

The characteristics of the area that the equipment will be expected to cover are critical factors that must be taken into account when selecting equipment. Designers or purchasers of security devices must know what area they are trying to protect, as well as what conditions may result in false alarms. Excessive false alarms resulting from any type of surveillance equipment can cause frustration among utility staff and ultimately result in discontinued use of valuable security equipment. Therefore, it is very important to consider false alarm rates in the design and purchase of electronic equipment. Selected equipment must have an appropriate sensitivity level that allows detection but is not triggered unnecessarily. Characteristics of both the equipment and the site conditions should inform these decisions.

Questions to consider include:

- What is the area or region to be protected?
- Does the area occupy a level surface?
- Is the area enclosed? Is the area indoors or outdoors? Indoor areas typically have lower nuisance alarm rates and are easier to protect.
- If indoors, what ambient noise levels, thermal conditions, or vibrations may exist?
- If outdoors, what humidity, temperature conditions, or wind conditions exist?
- Are small animals or children living nearby the protected space?
- How large is the area?
- What is the configuration and physical layout of the area protected?
- What are the existing lighting conditions within the area?
- Are any restrictions in place that limit placement or levels of site lighting, such as neighborhood zoning requirements?
- Are the assets visible from the fence or property line?

6.2.4 Levels of Resolution

To accurately specify the required security hardware, it is important to define the required level of resolution that the system must achieve: detection, classification, or identification.

- **Detection.** The capability to determine the presence of an intruder (but not necessarily classify as a human, animal, or object).
- **Classification.** The capability to determine the classification of an intruder as human.
- **Identification.** The capability to determine the identity of a human intruder.

6.2.5 System Size and Device Quantity

Before selecting equipment, it is also important for a utility to think about the size of the area that it wants to cover and the number of devices it will need. Understanding the potential growth needs of the system also allows the designer to provide a system that scales with a minimum of cost and effort as the system size and requirements expand.

6.2.6 Electrical Power, Wiring, and Transmission Methods

Availability of electrical power will also influence selection of security devices. Questions to consider include:

- What electrical power is available for security hardware, if any?
- What backup power is provided for security?
- Are lightning strikes a consideration? Is a lightning protection system advisable for new electronic equipment?
- Will all wiring be protected within conduit?
- How are alarm signals transmitted back to a monitoring system?
- Will hard-wired systems be used or are wireless communication methods being considered?
- What bandwidth is available for transmitting security alarms and video images? For example, dial-up telephone modems or radio telemetry systems provide limited bandwidth for transmitting video images, whereas high-bandwidth broadband connections allow higher rates of transmission and smoother video image playback.

6.2.7 Viewing, Assessment, and Alarm Response

Utilities also must consider how information transmitted by security devices will be used. Approaches to viewing and assessing camera images and responding to alarms should be part of the criteria when making decisions on equipment selection.

Questions for consideration include:

- What areas need surveillance? What camera surveillance systems may be required? Is there a need to have CCTV camera coverage at the entire site perimeter?
- What monitoring system is in place to receive the alarms: a SCADA system or a separate intrusion detection system? For example, it is advisable to separate the SCADA system from security alarms whenever possible so that an adversary cannot disable both simultaneously.
- Who will monitor the alarms? Will the alarms be monitored on a continuous basis or as alarms come in?
- Who will view the security alarms and assess them?
- Where is the monitoring system located?
- What is the security response once an alarm occurs?

- Is the response onsite or offsite?
- What is the response time?

6.3 Security Equipment

Once a utility understands the characteristics of the area to be protected and the security expectations and requirements, the utility can determine the type of security equipment to use. There are many different types of security equipment including:

- Intrusion detection (interior and exterior)
- Access control systems (card readers, PIN access, and biometrics)
- CCTV surveillance

Each of these types of security equipment is described in this section.

6.3.1 Interior Intrusion Detection

Many types of interior intrusion detection systems are in use today, including volumetric sensors and boundary penetration sensors.

6.3.1.1 Interior Volumetric Sensors

Volumetric sensors monitor an internal area to detect the presence of an intruder. There are several types of volumetric sensors, including microwave, ultrasonic, passive infrared (PIR), and dual-technology (microwave and PIR). The most commonly used are dual-technology sensors.

Dual-technology sensors use both microwave and PIR sensor circuitry within one housing. An alarm condition is generated if either the microwave or PIR sensor generates an alarm condition. In some dual-technology sensors, alarm settings may be adjusted to require that both the microwave and the PIR unit detect an intruder presence before an alarm condition is generated.

Small Utility Tip

Designs for smaller utilities might consider an exterior door contact and interior dual-technology sensor connected to a SCADA alarm point.

Dual-technology sensors have some drawbacks; for example, the PIR channel is relatively vulnerable. An elusive burglar may use an infrared emission-blocking cloak or screen to camouflage his infrared radiation. In addition, in hot climates when air-conditioning is off, there is a serious problem of misdetection with high ambient temperatures. Some dual-technology sensors attempt to overcome this limitation by having installer-selectable logic, where detectors from either channel are enough to trigger an event. However, this mode is not very popular because it suffers from the false alarm weaknesses of each technology.

6.3.1.2 Interior Boundary Penetration Sensors

Boundary penetration sensors detect the presence of an intruder across an interior boundary, such as a door, window, or hatch. The most typical boundary penetration sensors are door switches, glass-break sensors, and linear-beam sensors.

- **Door switches.** The workhorse of the security intrusion detection field, door switches include contact switches, magnetic switches, and balanced magnetic switches. These switches may be used in a variety of applications, from monitoring doors to monitoring hatches, vaults, and panel enclosures. By far, the most effective is the balanced magnetic switch. This switch has internal circuitry that resists tampering or defeat from strong magnetic fields. By comparison, standard magnetic switches have been defeated by applying a strong magnet to the exterior of the door to bypass an alarm and force the door open.
- **Glass-break sensors.** There are three basic types of glass-break sensors: acoustic sensors (listens for an acoustic sound wave that matches the frequency of broken glass), shock sensors (feels the shock wave when glass is broken), and dual-technology sensors (senses acoustic and shock vibrations). Because glass-break sensors do not sense motion or intrusion from entering a door or hatch, the sensors should be used in conjunction with other methods (such as volumetric sensors). It is recommended that glass-break sensors not be placed directly on a glass surface.
- **Linear-beam sensors.** Also referred to as a photoelectric beam or photoelectric eye, linear-beam sensors consist of a transmitter that emits a beam of light that is invisible to the human eye and a receiver that receives the beam of light. If the beam of light is interrupted or broken by motion from an intruder, an alarm is triggered. Linear beam detectors can be surface mounted or recessed. These sensors require a straight line of sight between the transmitter and the receiver.

6.3.2 Exterior Intrusion Detection

Several types of exterior intrusion detection sensors exist and may be classified according to type, method of use, style, and mode of application. The following exterior systems are most applicable to wastewater system applications: freestanding sensors, buried-line sensors, and fence-mounted sensors.

6.3.2.1 Freestanding Sensors

Freestanding sensors are the most common style of exterior sensor available. Types include active infrared, PIR, microwave, and dual-technology sensors. Microwave and dual-technology detectors are frequently used as freestanding sensors and are discussed below.

Small Utility Tip

Monostatic microwave sensors work well for monitoring reservoir ladders or other small areas. The device can be aimed down a reservoir ladder toward the ground, for example. Make sure the device is rated for outdoor use before installing.

- **Microwave sensors** come in two styles: bistatic and monostatic. Bistatic microwave sensors use a transmitter and receiver pair. Monostatic microwave sensors use a single sensing unit that incorporates both transmitting and receiving functions. With both bistatic and monostatic sensors, the sensors operate by radiating a controlled pattern of microwave energy into the protected area. The transmitted microwave signal is received, and a base level “no intrusion” signal level is established. Motion by an intruder causes the received signal to be altered, setting off an alarm. Microwave signals pass through concrete and steel and must be applied with care if roadways or adjacent buildings are near the area of coverage, otherwise nuisance alarms may occur. Many monostatic microwave sensors feature a cut-off circuit, which allows the sensor to be tuned to cover only a selected region to reduce nuisance alarms.

- **Dual-technology sensors** use a combination of PIR and microwave technology, as discussed previously.

6.3.2.2 Buried-line Sensors

Buried-line sensors include pressure/seismic sensors, magnetic field sensors, buried-ported coaxial cable, and buried fiber-optic cable sensor systems. Each of these systems relies on sensing the presence of an intruder by means of a buried cable system within the ground.

A factor that must be considered when using buried-line sensors is the presence of underground utilities. Underground utilities, such as gas, water, and sewer lines, must be sufficiently below the detection zone, or false alarms may result. Typically, 1 meter (3 feet) is sufficient to prevent false and nuisance alarms. Underground electrical wires must also be considered.

Other factors must also be considered when using a buried-line sensor. Rodents have been known to cause maintenance problems by gnawing on the sensor cables. Installations also should not be in areas where running water will either wash away the soil that buries the sensor, cause nuisance alarms during a heavy rain, or result in any standing water or pooling issues.

A drawback to the buried-line sensor system is that it may have different sensitivities when buried below different surfaces. For example, if a continuous system is buried below a concrete surface as well as under a lawn, the sensitivities required for each surface may be different. A good sensitivity adjustment for concrete may be too sensitive for grass. In this case, it may be best to individually zone those areas, so that the sensitivities may be adjusted for each area.

6.3.2.3 Fence-mounted Cabling Sensors

With all fence-mounted systems, it is critical that the fence construction be of high quality, with no loose fabric, flexing, or sagging material. The fence should also have solid foundations for posts and gates. Otherwise, nuisance alarms may occur.

Several types of fence-mounted perimeter intrusion detection systems exist. These include electro-mechanical vibration sensing, coaxial strain-sensitive cable, fiber-optic strain-sensitive cable, and taut-wire systems. Two styles of fence-mounted sensors are most prevalent and are described below: coaxial and fiber-optic fence sensing.

Small Utility Tip

Fence-mounted sensor systems work well in areas without animals or passersby; otherwise, nuisance alarms may result.

- **Coaxial strain-sensitive cable systems** use a coaxial cable woven through the fabric of the fence. The coaxial cable transmits a dielectric field. As the cable moves due to strain on the fence fabric caused by climbing or cutting, the electric field changes are detected within the cable, and an alarm condition occurs.

- **Coaxial strain-sensing systems** are readily available and are highly tunable to adjust for field conditions due to weather and climate characteristics. Some coaxial cable systems are susceptible to electromagnetic interference and radio frequency interference.
- **Fiber-optic strain-sensitive cable systems** are similar to the coaxial strain-sensitive cable systems. The fiber-optic system uses a fiber-optic cable, rather than a coaxial cable, woven through the fence fabric. Strain on the fence fabric causes micro-bending of the fiber cable, which is monitored by the control panel, generating an alarm condition.
- **Fiber-optic strain-sensing systems** are relatively newer detection systems but have a strong following. The systems are readily available and are highly tunable to adjust for field conditions due to weather and climate characteristics. The systems are impervious to lightning, electromagnetic interference, radio frequency interference, or other electronic signals and can be used over long distances.

Possible defeat measures include tunneling, jumping, or bridging across the fence system. Careful climbing at corner posts may not generate sufficient vibration to generate an alarm condition.

6.3.3 Access Control

An access control system allows the movement of authorized personnel and material into and out of facilities while detecting and possibly delaying movement of unauthorized personnel or contraband. Entry control elements may be found at a facility boundary or perimeter, such as at vehicle gates, building entry points, or doors into rooms or other special areas within a building.

Access control systems make a verification decision and then determine whether to grant or deny access to a person. This verification decision is usually based on determining whether the person:

- Carries a valid credential, such as an access card.
- Knows a valid PIN.
- Possesses the proper unique physical characteristic that matches the person's characteristic recorded at enrollment. This is called biometrics and includes characteristics such as a fingerprint or hand geometry.

These three concepts are summarized as "what you have," "what you know," and "who you are" and are described in the following subsections. It is important to remember the effectiveness of any access control system is improved significantly through basic security policies such as key control and a cultural emphasis on security. Suggestions on security policies and management concepts are presented in Section 2 of this document.

6.3.3.1 Credentials (Access Card Types)—What You Have

There are a number of different types of credentials (or access cards) used in personnel entry control, including photo identification, exchange, stored-image badges, and coded credentials. There are many techniques available for coding a badge or card. The most common techniques include magnetic stripe, Wiegand wire, bar codes, proximity, and smart cards. Eighty percent of the card reader market uses magnetic stripe, Wiegand wire, or proximity technology.

Card reader access control systems provide the most reliable, flexible method of controlling access to a facility. Card reader systems come in many configurations, from stand-alone systems controlling only one door to scaleable systems to provide enterprise-wide control for an entire corporation spanning multiple continents. Newer card reader systems offer sophisticated database intelligence that allows integration with payroll, information technology, and human resources databases. If an employee is terminated, his or her access privileges can be revoked within the access control system instantaneously. Some access control systems offer seamless integration with video surveillance systems, where access control alarms and video surveillance images are displayed on common PC workstations.

As shown in Exhibit 6-1, a card reader system typically consists of:

- A computer server or workstation that displays alarm conditions and allows programming of the system
- A badge station, allowing creation and programming of badges
- Local control panels that control the doors, card reader units, and access cards
- A printer unit that prints each event and alarm condition

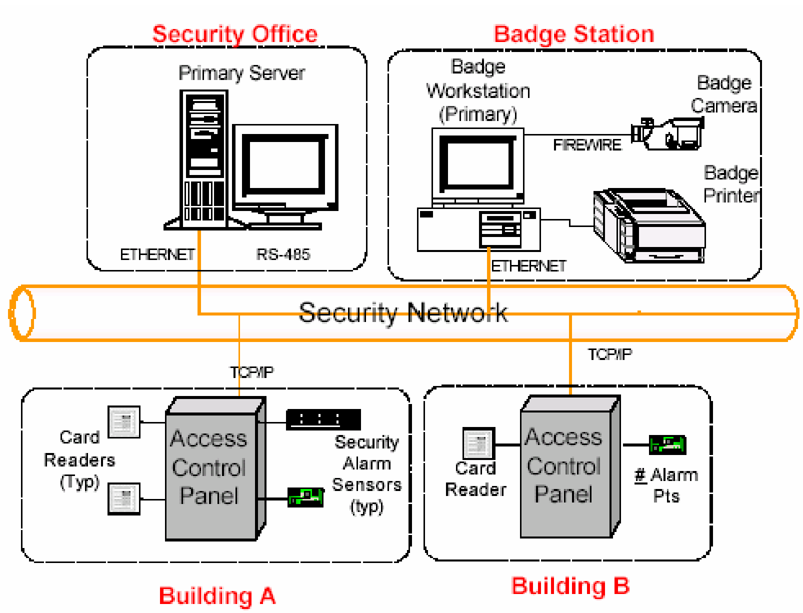

EXHIBIT 6-1
Typical Card Reader System

Under normal operation, the system grants access at doors with card readers by comparing the time and location of any attempted entry with information stored in memory. Access is granted only when the security card used has a valid entry code at the card reader for a designated time frame.

Significant advantages of the card reader system include the capability for event tracking and programmable software functions, such as the following:

- **Event tracking/event logs** are logs of security events recorded by the access control system that indicate the actions performed. Each event log entry contains the time, date, and other information specific to the event.
- **Two-man rule software** is software programming that is optional on many card reader systems. It prevents an individual cardholder from entering a selected empty security area unless accompanied by at least one other person or exiting if only one person will remain in the area. Once two cardholders are logged into the area, other cardholders can come and go individually as long as at least two people are in the area. Conversely, when exiting, the last two occupants of the security area must exit together.
- **Anti-passback software** prevents users from giving their cards to someone else to use. This feature is sometimes available with keypads. To prevent the same PIN from being used by many people, a time element can be programmed in so that the PIN will not work after the first time until a specified time expires. Some anti-passback systems require that, if a card is used to enter an area, the same card must be used to exit that area before it can be used to gain access to a different or unrelated area. This feature also helps eliminate "piggy-backing" or tailgating by unauthorized persons.

6.3.3.2 PIN—What You Know

There are two primary considerations for selecting a secure PIN. First, the PIN should be long enough and have enough digits to prevent easy guessing, i.e., at least 6-digits in length. The PIN should be a combination of letters (with capitalization), numbers, and characters for better security. Second, the PIN should not be a number that is too meaningful to the individual to whom it is assigned (e.g., birthday or nickname). If a person is allowed to choose his or her own PIN, he or she should be discouraged from choosing a PIN that is too meaningful. These considerations are consistent with the concept of strong authentication for computer passwords discussed in the Section 5 of this document.

Some systems provide a maximum number of PIN entry attempts before disallowing the credential or generating an alarm to the central control system.

6.3.3.3 Biometrics—Who You Are

Commercial equipment is available that uses hand or finger geometry, handwriting, eye pattern, fingerprints, speech, face, and various other physical characteristics to identify an individual. When selecting or deploying biometric devices, consideration of the security objectives is required to assure that the optimal device is selected and that it will operate as desired.

Hand readers and fingerprint readers are the most common biometric access control applications. Fingerprint reader stations are physically smaller in size and have a lower cost than hand geometry readers. Fingerprint readers are best suited for installations with smaller user populations (such as a lab area accessed by approximately 20 people), whereas larger user populations are better served by hand geometry readers.

Not everyone can use biometric devices. Fingerprint readers have a higher false-rejection rate than do hand geometry readers. For example, a portion of the population cannot use fingerprint readers because of dry skin. Manual labor staff who routinely use their hands may have worn fingerprints or scars on their fingertips, making it difficult for effective fingerprint reading. In addition, physical changes occur with age or injury that can impact biometric reader effectiveness. In these cases, a hand geometry reader might be a more effective technology.

Training on the capabilities and limitations of the selected biometric device is essential. The procedures need to provide for the periodic update of biometric data for each person tracked by the device; enrollment of staff into a biometric reader is not a one-time actions.

6.3.4 CCTV Camera Systems

CCTV camera surveillance systems are integral to effective assessment of alarms. This section describes some of the requirements and components comprising a CCTV system.

As shown in Exhibit 6-2, a CCTV system typically consists of:

- one or more cameras
- transmission media (fiber cable, coaxial, or twisted-pair cabling)
- a monitor for viewing incoming camera images

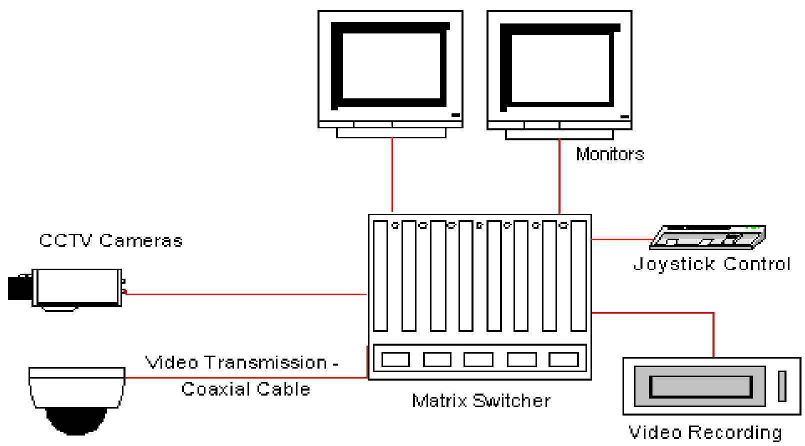

EXHIBIT 6-2
Typical CCTV System

- a matrix switcher or multiplexer that receives incoming video streams and directs them to monitors and recording equipment
- a means to record each event and alarm condition

6.3.4.1 Camera Characteristics

There are several key performance characteristics of a video surveillance camera. Among these are:

- **Camera Resolution.** The amount of detail that the camera can distinguish and produce.
- **Minimum Illumination.** The minimum amount of light needed for the camera to display images. (For illumination, the lower the number, the better.)
- **Lenses.** The lens size and type required for the camera.

Other important considerations of CCTV camera systems are whether the cameras are fixed or pan, tilt, and zoom (PTZ) cameras:

- **Fixed-position Camera Mounts.** The camera is mounted in a fixed position and cannot rotate or pan. A good application for fixed cameras is *detection* surveillance, because video motion detection can be more readily applied to the static field of view.
- **PTZ Camera Mounts.** These camera mounts allow the camera to rotate, pan, tilt, and zoom. Because of the drive motor and housing, PTZ cameras are typically four times more expensive than fixed cameras. PTZ cameras are often used for *assessment* surveillance applications to view and assess alarm conditions.

Other camera features include the following:

Matrix switchers are components that provide switching capability between cameras and viewing monitors. They typically offer functionality that allows programmable settings such as camera naming, guard-tour camera sequences, and salvo switching.

Digital video recording provides a great improvement in camera image storage. Benefits include eliminating consumable media (tapes), reducing physical storage space, ease of search-and-playback functions, and the capability to add watermarks for documenting evidentiary recordings.

Video motion detection systems permit detection of entry or intrusion using video images. This new technology is based on computer algorithms that analyze the received video image and compare it to stored images in the system memory. The incoming video is analyzed for the direction of the object's movement and changes in images and background "texture." Advanced software can also distinguish between human, non-human, and vehicle images and initiate appropriate alarms.

6.3.4.2 Low-light Cameras

Several technology solutions are available to permit viewing under low light conditions, including black/white switching cameras, infrared illuminators, or thermal imaging cameras.

- **Color - black/white switching.** Some cameras will automatically switch from color during daytime to black/white at night, which permits viewing under low light conditions. This can be an effective solution in situations where the existing illumination levels are too low during night conditions to permit color camera use, but color camera use is desired during daytime conditions. Numerous CCTV camera manufacturers offer auto-switching black/white cameras.
- **Infrared illuminators**. The human eye cannot see infrared light. Most mono-CCTV cameras, however, can. Thus, invisible infrared light can be used to illuminate a scene, which allows night surveillance without the need for additional artificial lighting. Infrared also provides many other benefits above conventional lighting, including:
  - IR beam-shapes can be designed to optimize CCTV camera performance.
  - Extended bulb-life.
  - Covert surveillance, no visible lighting to alert or annoy neighbors.
  - Lower running costs.

It is important to design illumination specifically for the CCTV camera being used. The range that the camera will see in the dark depends on sensitivity and spectral response of the camera and lens combination.

A number of camera manufacturers each produce a variety of beam patterns, e.g., 10 and 30° spot (precise) illuminators and 60° flood illuminators.

- **Thermal imaging** cameras use special technology that senses heat signatures rather than visual information. These cameras operate under complete darkness. Thermal imaging cameras are best used in long-range detection and surveillance applications. Because they register a heat signature, it is not possible to resolve the *identification* of the adversary; instead, these cameras are best used to indicate the *presence* of an adversary.

6.3.4.3 CCTV System Recommendations

Considerations when purchasing a CCTV system include:

- Ask the dealer if the new system or device is compatible with any existing devices such as cameras, matrix switches, and multiplexers. Rewiring for new cameras and devices is labor-intensive and can be expensive.
- Look for ease of use.
- Investigate the scalability of the system. If more cameras are needed locally or remotely, can new systems be added with as little effort as possible?
- Understand the service plan. Manufacturers provide service and maintenance programs, and some have premier service plans that provide feature upgrades and enhancements on computer-based video recorders.
- Consider how the images will be viewed, the number of monitors needed to support the system, and how multiple camera scenes will be multiplexed onto a common monitor (not every camera requires an individual monitor).
- Integrate an incident alarm feature into the CCTV system so that continuous monitoring is not required. Some type of notification (e.g., an alarm on the CCTV monitor or SCADA control screen) linked to detection should trigger an operator or security professional to assess an alarm. A well-designed Security Control Room may have only one or two monitors that display continuously and 2 others that are blank until an event them, at which time the operator is alerted. Cameras should all be linked to sensors that automatically bring them up to monitor. Let the machine do what it does best—detect, and let the humans do what they do best—respond and evaluate.

Considerations when implementing a CCTV system include:

- The main concern with remote video monitoring is data security. Unless adequately protected, it may be possible for a hacker to gain access to remote video sites. To reduce the possibility of unauthorized access, user name and password protection is an important feature that must be implemented. A firewall and video encryption should also be employed to dramatically reduce the chance of unauthorized entry into the system.
- Use ample light whenever possible. The most common reason for poor quality images is that the light level is too low. Generally, the more light, the better the images. With lighting levels too low, images become noisy and blurry with dull colors. For low-light situations, ensure that you have a low-light camera.
- Scene illumination should be even across the field of view of the camera, with a maximum light-to-dark ratio of 8 to 1. The minimum illumination level should be 11 lux (one footcandle).
- Avoid backlight. Try to avoid bright areas in the images. Bright images might become over-exposed (bright white) and objects might appear too dark. This problem typically occurs when one tries to capture an object in front of a window.
- Reduce the contrast. A camera adjusts the exposure to obtain good average light level in the image. A person in front of a white wall tends to appear too dark. If a gray wall is used instead, this problem does not exist.
- Sensor size. The lens must make an image large enough for the sensor. The larger the sensor, the more expensive the lens. If a lens made for a smaller sensor is used on a bigger sensor, the image will have black corners.
- Lens and field of view. The lens selection and alignment should be established so that a reasonable width of the alarm sector can be seen at the near field of view. The far field of view should be no more than 41 meters (135 feet) wide at the far end of the alarm sector to allow at least 4.5 pixels to cover a 0.3 meter (1-foot) square target. This minimum resolution is needed to classify the intrusion source as being a person versus an animal or debris, and requires that the camera be mounted several meters outside the zone being assessed.
- Focal length. Wide-angle lenses have a better depth of field than telephoto lenses. This means that you can focus both close to the camera as well as at a distance. Telephoto lenses require a more precise focus adjustment.
- Iris. Always use auto-iris lenses for outdoor applications. The iris automatically adjusts the amount of light reaching the camera and thereby optimizes its performance. The iris also protects the image sensor from getting damaged by strong sunlight. With an auto-iris lens, always set the focus in low light. If the adjustment is made in sunlight, it is very easy to focus, but then at night the iris diameter increases and the image is not in focus anymore. Special dark focus filters are available that reduce the light up to ten times.

6.3.4.4 Mounting a Camera Outdoors

When mounting a camera outdoors, the lighting changes depending on the time of day and the weather. Because of this, consider the following for outdoor cameras:

- As discussed previously, always use auto-iris lenses with outdoor cameras.
- Use caution when mounting a camera behind glass. If you mount a camera behind glass, such as in housing, make sure that the lens is close to the glass. If the lens is too far away from the glass, reflections from the camera and the background will appear in the image.
- The mounting height for the camera should be high enough to angle the camera down to avoid sunglare, yet low enough so that no lamps are visible in the camera field-of-view.
- Avoid direct sunlight. Direct sunlight blinds the camera and may permanently bleach the small color filters on the sensor chip, causing stripes in the image. If possible, position the camera so that it is looking in the same direction as the sun.
- When using a camera outdoors, avoid viewing too much sky. Due to the large contrast, the camera will adjust to achieve a good light level for the sky, and the interesting landscape and objects might appear too dark. One way to avoid these problems is to mount the camera high above ground. Use a pole if needed.
- Always use sturdy mounting equipment to avoid vibrations caused by strong wind. Wood poles should not be used for cameras, and the use of cantilevered-arm mounts or poles is discouraged because of stability concerns in wind. Metal triangular antenna tower sections are ideal for stability.

6.3.4.5 CCTV Compression Standards

Digital images and digital video are always compressed to save space on hard disks and make transmission faster. Typically, the compression ratio is 10 to 100. An uncompressed image with a resolution of 640 x 480 pixels is approximately 600K (kilobytes) (2 bytes per pixel). Compressed 25 times, the image is approximately 25K. There are a number of common compression standards:

- Joint Photographic Experts Group, more commonly known as **JPEG,** is a good and very popular standard for still images that modern programs support. This is the preferred standard for many network cameras. The JPEG compression ratio is approximately 10:1.
- **Motion-JPEG** is a variation of JPEG where still images are shown at a high frame rate. It gives very high-quality video, but unfortunately, it consists of a lot of data, with a compression ratio of approximately 20:1.
- Moving Picture Experts Group **(MPEG) 2** is a standard for video. Many variations are possible, but normally MPEG 2 performs at 720 x 480 pixels, 30 frames—per-second. Only modern computers (Pentium III with adequate random access memory [RAM]) can decode MPEG 2, as it requires larger computing capacity. The compression ratio is approximately 20:1 or better.
- **MPEG 4** is a new standard for video. It provides better performance than MPEG 2, but it is not commonly used. Compression ratios for MPEG 4 can be 200:1 or better.

6.3.4.6 Example System Performance Criteria

- CCTV cameras and fields of view are configured such that the area of interest (face, license plate, etc.) occupies a certain percentage of the overall width of the scene.
- For cameras used for *detection* of an intruder (i.e., the capability to determine the presence of an intruder, but not necessarily classify as a human, animal or object), the area of interest should occupy a minimum of 10 percent of the field of view, with a maximum field of view of 91 meters (300 feet) in length or less.
- For cameras used for *classification* of an intruder (i.e., the capability to determine the classification of an intruder as human), the area of interest should occupy a minimum of 15 to 20 percent of the field of view, with a maximum field of view of 61 meters (200 feet) in length or less.
- For cameras used for *identification* of an intruder (i.e., the capability to determine the identity of a human intruder), the area of interest should occupy a minimum of 25 percent of the field of view, with a maximum field of view of 23 meters (75 feet) in length or less.
- All CCTV cameras shall be listed in accordance with Underwriters Laboratories (UL) 3044, Surveillance Closed Circuit Television Equipment.
- Exterior cameras should have minimum resolution of 470 horizontal lines.
- Exterior cameras should be rated for use at 0.54 lux (0.05 foot-candles).
- The camera should provide adequate onsite digital recording capacity for all cameras at 30 days of continuous storage at 1 frame per second.
- CCTV equipment should have integral digital video motion detection capabilities. The system should be programmable to degree of motion, range of motion, speed, number of pixels to cause motion, and area of motion detected.
- To conserve bandwidth and storage requirements, the CCTV equipment should be capable of providing a video compression ratio of 20:1 (or better).

6.3.5 Visibility and Lighting Recommendations

Visibility and lighting are critical elements of a successful security system.

6.3.5.1 Visibility

Within a parking lot, trees and shrubs should not obstruct viewing. Tree branches and leaves should not be lower than 3 meters (10 feet) above the lot surface. Interior shrubs and bushes should not be higher than 46 centimeters (18 inches) so as not to obstruct vision or conceal an adversary.

6.3.5.2 Lighting

A significant part of visibility is lighting. Lighting should enable people parking and employees to note individuals at night at a distance of 23 meters (75 feet) or more and to identify a human face at about 10 meters (33 feet). These are distances that will allow them, if necessary, to avoid the individuals or take defensive action while still at a safe distance.

Security lighting increases the effectiveness of guard forces and closed circuit television by increasing the visual range of the guards or CCTV during periods of darkness. It also provides increased illumination of an area where natural light does not reach or is insufficient. Lighting also has value as a deterrent to individuals looking for an opportunity to commit crime. Normally, security lighting requires less intensity than lighting in working areas. An exception is at normal doorways.

Exterior lighting for areas such as parking lots ensures a minimum level of visibility when guards perform inspection of the protected area. Guards and CCTV surveillance systems must be able to:

- see badges, people, and other guards at gates
- observe activity
- inspect vehicles
- observe illegal entry attempts
- detect intruders in the protected area
- observe unusual or suspicious circumstances

Each parking lot presents its own particular problems based on physical layout, terrain, atmospheric conditions, and security requirements. The goals of direct illumination are to provide a specified intensity throughout the area for support of guard forces or CCTV, provide good visibility for customers or employees, and have a minimum of glare.

The most severe problem is illuminating the small narrow "corridors" formed by adjacent parked cars. To get light into these areas, it is recommended that any point in the entire parking lot be provided with illumination from at least two and preferably four lighting (pole) locations. The lights should be mounted at a minimum height of 6 meters (20 feet), with the lowest value of illumination on the pavement not less than one-fourth of the recommended average (a 4:1 light-to-dark ratio).[23]

6.3.5.3 Example System Performance Criteria

The minimum recommended illumination levels for the barest sight essentials on the parking lot are:

- Provide lighting that is a minimum of 2.2 lux (0.2 foot-candles) around key assets for observation by unaided eye.
- Provide minimum of 2.2 lux (1 foot-candle) (the average maintained horizontal to the surface) for self-parking areas.
- Lighting at entry and exit points should be at least 16 to 22 lux (1.5 to 2.0 foot-candles) for safety and for adequate observation by employees or CCTV.
- Twenty-two lux (2 foot-candles) of lighting should be provided for attendant parking areas because of liability and potential damage to automobiles.
- Where additional lighting is required, lighting of 54 lux (5.0 foot-candles) and higher is often used.

Small Utility Tip

Low pressure sodium lights are reasonably efficient and provide a uniform lighting ratio.

[23] RP-20-98, *Lighting for Parking Facilities*, Illumination Engineering Society of North America

- RP-20-98, Lighting for Parking Facilities, published by the Illumination Engineering Society of North America, provides recommended illumination levels for parking facilities.

6.3.6 Power and Wiring

Without a reliable power source and intact wiring, a security system cannot function. Indeed, cutting the power to a security device may be an adversary's first course of action. Recommendations for reliable power and security wiring are presented here.

6.3.6.1 Uninterruptible Power Supplies and Battery Backup

For all electronic components of the security system, some method of power backup is recommended. With generator-backed systems, if normal AC power fails, there is a 5- to 10-second lag before generator backup engages. With manual systems this time can be much longer. Thus, uninterruptible power supply (UPS) systems are recommended for devices requiring 120V ac power, such as computers and video monitors.

When considering UPS systems, compare the cost and flexibility of using smaller point-of-use UPS units against a large system-wide UPS. In some cases, greater flexibility and cost-effectiveness may be achieved using point-of-use UPS units. Additionally, the cost of maintaining a spare point-of-use UPS unit is much lower then providing a redundant system-wide standby UPS unit.

Batteries are cost-effective and reliable for low-voltage devices, such as cameras and card reader systems. Four-hour battery backup is recommended, at a minimum. Provide automatic charging means to automatically maintain battery charge under normal power conditions, and provide recharging means to automatically recharge batteries within 24 hours after charged batteries have been discharged. Provide extra protection for single-point-of-failure equipment such as the power transfer switch for backup power.

Modular battery backup systems provide an advantage because they may be expanded by simply adding more components and batteries. As backup power requirements increase, the battery system capacity can be adjusted to meet current needs.

6.3.6.2 Security Wiring

Recommendations for the wiring of security devices are as follows:

- All exposed security wiring should be installed in conduit. The wiring conduit should be concealed, where possible within the structure.
- No splices or wire nuts should be used within wiring circuits. All wiring terminations should be made via mechanical termination blocks.
- All interconnecting wiring between security system components should be monitored for integrity so that an abnormal condition (wire-to-wire short, wire break, or wire ground-fault condition) is automatically indicated to the user upon arming the system or causes an alarm if the system is already armed.

- Coaxial cable RG-59U, the most common coaxial cable style is rated for up to 229 meters (750 feet). Use fiber-optic cable for CCTV runs farther than 229 meters (750 feet).
- Fiber optic cable offers several advantages over coaxial cable; it is impervious to electromagnetic interference, radio frequency interference and offers good security against eavesdropping. For new CCTV installations, fiber is recommended over coaxial cable, except for very short runs (under 15 meters [50 feet]).

6.3.6.3 Example System Performance Standards

- All wiring shall comply with the NFPA 70, National Electrical Code, specifically Articles 725 and 800, as appropriate.
- Security panels shall be UL listed as meeting standard UL804.

6.4 Summary

A variety of different security systems and components are commercially available. Before implementing a security system, it is important to understand the characteristics and requirements of the area and facility to be protected. With this understanding, detailed and specific criteria can be developed to specify exactly how the security system should be implemented.

Technology and manufacturers of security devices are rapidly changing. Therefore, web resources are useful for getting the latest information on security products. USEPA has published guidance for water and wastewater utilities on security devices and equipment in the form of its Security Product Guides. This guides are kept up-to-date on EPA's web site at www.epa.gov/safewater/security under the Primary Topic of "Security Enhancements, Research, and Technology." At the time of writing, guides are available for security products, cyber protection products, physical asset monitoring products, and water monitoring products. At the time of writing, guides are available for security products, cyber protection products, physical asset monitoring products, and water monitoring products.